REMARKS

Claims 1-5 are pending in this application, with claim 1 being the only independent claim. Claims 1-5 have been amended. The title of the invention has been objected to for not being descriptive. The drawings have been objected to for various errors. Claim 5 has been objected to because the recitation of "n=3" lacks antecedent basis. Claims 1-3 have been rejected under 35 U.S.C. §103(a) as unpatentable over U.S. Patent 5,850,444 (Rune), in view of U.S. Patent 4,644,368 (Mutz), and further in view of U.S. Patent Appln. Pub. 2004/0063438 (Hsu). Claims 4-5 have been rejected under 35 U.S.C. §103(a) as unpatentable over Rune, Mutz, and Hsu, and further in view of U.S. Paten 7,308,573 (Kostal).

Claim of Foreign Priority

Applicants include a certified translation of the foreign priority document herewith.

Objection to the title of the invention

The Office Action states that the title of the invention has been objected to for not being descriptive. The title of the invention has been amended to be more descriptive. Applicants submit that this objection has been overcome.

Objection to the drawings

The Office Action states that TDES is misspelled in step 13 of Fig. 1, and a left to right arrow is missing from T2 to T1 in Fig. 2. Fig. 1 has been amended to correct the misspelling. Fig. 2 has been amended to include the left to right arrow between T2 and T1.

Applicants submit that these objections have been overcome.

Objection to claim 5

The Office Action states that claim 5 has been objected to because the recitation of "n=3" lacks antecedent basis. Claim 5 has been amended to depend from claim 4, and now has proper antecedent basis.

Rejection of claims 1-3 under 35 U.S.C. §103(a)

The Office Action states that the combination of Rune, Mutz, and Hsu teaches all of Applicants' recited elements. Applicants disagree and submit that the combination of Rune, Mutz, and Hsu is improper.

Applicants invention is directed to a method for secure data transmission between a first subscriber and second subscribers. The first subscriber is a tachograph in a commercial vehicle and the second subscribers are memory cards having at least one respective data store. The first subscriber has a memory, which stores a particular number of entries each comprising identifiers and associated security certificates from second subscribers with a detection time for the security certificate. Applicants' recited method includes fetching an identifier by the first subscriber from a second subscriber that is connected to the first subscriber, and comparing by first subscriber the fetched identifier with the identifiers stored in the memory. According to Applicants' recited method, if a matching identifier is present in the memory, the security certificate associated with the identifier is prompted to be a basis for a subsequent data transmission and updating the detection time for the security certificate is updated to a current system time. If no matching identifier is stored in the memory, the first subscriber is prompted to perform security certificate verification with the connected second subscriber and, in the event of verification, an entry

corresponding to the verified security certificate with a current detection time is stored in the memory. The entry with the oldest detection date is replaced by the new entry if a particular number of entries has already been reached.

Thus, the purpose of Applicants' recited invention is to reduce the time required for the security certificate verifications for the subscribers involved in the data interchange without losing protection against manipulation.

The rejection of independent claim 1 is a combination of references. With respect to combinations of references, MPEP §2143 cites the Supreme Court's *KSR* decision and states as follows:

The rationale to support a conclusion that the claim would have been obvious is that all the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination yielded nothing more than predictable results to one of ordinary skill in the art. *KSR*, 550 U.S. at ___, 82 USPQ2d at 1395; *Sakraida v. AG Pro, Inc.*, 425 U.S. 273, 282, 189 USPQ 449, 453 (1976); *Anderson's-Black Rock, Inc. v. Pavement Salvage Co.*, 396 U.S. 57, 62-63, 163 USPQ 673, 675 (1969); *Great Atlantic & P. Tea Co. v. Supermarket Equipment Corp.*, 340 U.S. 147, 152, 87 USPQ 303, 306 (1950). "[I]t can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does." *KSR*, 550 U.S. at ___, 82 USPQ2d at 1396.

As will be described below, (1) one skilled in the art could not have made the combination proposed by the Examiner by known methods with no changes in their respective functions, and (2) such a combination does yield the presently claimed invention.

The Examiner cites Rune as teaching Applicants' recited method of secure transmission. Rune discloses a method and apparatus for encrypting radio traffic in a telecommunications network. According to Rune, a generic communications network provides an encrypted communications interface between service networks and their subscribers. When communications are initiated between a subscribing communications terminal and the generic network, the terminal compares a stored network identifier associated with a stored public key, with a unique identifier broadcast by the generic network. If a match is found, the terminal of Rune generates a random secret key, encrypts the secret key with the stored public key, and transmits the encrypted secret key. The generic communications network of Rune decrypts the secret key using a private key associated with the public key. The secret key of Rune is used thereafter by the terminal and the generic network to encrypt and decrypt the ensuing radio traffic. Consequently, the network can maintain secure communications with the terminal without ever knowing the terminal's identity (see Abstract of Rune).

The network in Rune communicates with a plurality of subscriber terminals. Similarly, the first subscriber tachograph communicates with a plurality of second subscriber memory cards. Thus, the network of Rune is analogous to the first subscriber tachograph. Rune teaches that the subscriber terminals maintain a list of networks. Accordingly, Rune fails to teach or suggest "comparing by the first subscriber the fetched identifier with the identifiers stored in the memory", as expressly recited in independent claim 1

Even if the subscriber terminal of Rune is considered to be the claimed first subscriber (tachograph), which applicants do not believe to be true, Rune teaches that a secret key is generated when a match is found. Thus, Rune also fails to teach or suggest "if a matching identifier is present, prompting the security certificate associated with the identifier to be a basis for a subsequent data

transmission and updating the detection time for the security certificate to a current system time", as expressly recited in independent claim 1.

Rune is concerned only with encrypting radio traffic between a terminal and a general access network (GAN), and neither teaches nor suggests providing secure communication between a tachograph and a memory card located in a vehicle, or that such an encrypted communication network would or could be used with small scale devices, such as a tachograph and memory card.

The Examiner concedes that Rune fails to teach or suggest a tachograph and memory cards, a detection time for the security certificate, updating the detection time for the security certificate to a current system time, storing, in the event of verification, an entry corresponding to the verified security certificate with a current detection time in the memory, and replacing the entry with the oldest detection date by the new entry if a particular number of entries has already been reached, as recited in Applicants' claim 1.

The Examiner cites Mutz as teaching a tachograph and a memory card, and asserts that it would have been obvious for one skilled in the art to combine the communication method of Rune with the tachograph of Mutz to achieve a tachograph that provides secure communication between the tachograph and a memory card. Applicants disagree.

Mutz discloses a tachograph that writes work data for motor vehicle work into a microprocessor-controlled EEPROM semiconductor memory mounted on a movable data card carried by the driver (see Abstract of Mutz). The purpose of the device of Mutz is to provide a tachograph that to avoids the deficiencies of diaphragm disk recording, but which can receive driver-directed data carriers enabling changes of driver and vehicle in a manner analogous to conventional driving data acquisition devices, and which at all times permits a correct clock time or real time drive data output without requiring additional technical evaluation expenditure for its

interpretation (see col. 2, lines 50-59 of Mutz). There is no reason to apply the encrypted communication method of Rune with a tachograph/memory card combination such as disclosed by Mutz.

Furthermore, such a combination does not disclose, teach or suggest "comparing by first subscriber the identifier with the identifiers stored in the memory" and "if a matching identifier is present, prompting the security certificate associated with the identifier to be a basis for a subsequent data transmission and updating the detection time for the security certificate to a current system time", as expressly recited in independent claim 1.

Because Rune relates to encrypted communication and is not concerned with secure data transmission on a small scale between device in a vehicle (i.e., between a tachograph and an inserted memory card), and because Mutz is only concerned with achieving a better recording of data, there is no motivation for one skilled in the art to look to the method of Rune as means for providing a secure transmission between the tachograph and data card of Mutz. The Examiner has found motivation to combine only through the disclosure of Applicants' invention, which is impermissible hindsight.

Furthermore, the result of combining the communication method of Rune, which is intended for secure communication between a terminal and a general access network, with small scale devices such as a tachograph and a data card of Mutz does not yield predictable results.

Hsu fails to teach what Rune and Mutz lack. The Examiner cites Hsu as teaching a detection time for the security certificate, updating the detection time for the security certificate to a current system time, storing, in the event of verification, an entry corresponding to the verified security certificate with a current detection time in the memory, and replacing the entry

with the oldest detection date by the new entry if a particular number of entries has already been reached, as recited in Applicants' claim 1.

Hsu discloses a point to multipoint wireless communication system that includes an access point having an antenna, a processor, and circuitry in communication with the access point antenna and controlled by the access point processor to transmit wireless electromagnetic signals to, and receive wireless electromagnetic signals from, an area. Hsu is concerned only with providing an improved wireless point to multipoint communication system (see paragraph [0004] of Hsu).

Further, Hsu teaches storing in a memory a list of subscriber units that associates user devices with the subscriber units. The list of Hsu is maintained by an access point for all the subscriber units in the access point's center. The list disclosed by Hsu has nothing to do with a tachograph memory storing driver card identifiers. Even if the teaching of Hsu were combined with Rune and Mutz, the combination fails to teach or suggest " "comparing by first subscriber the identifier with the identifiers stored in the memory" and "if a matching identifier is present, prompting the security certificate associated with the identifier to be a basis for a subsequent data transmission and updating the detection time for the security certificate to a current system time", as expressly recited in independent claim 1.

In view of the foregoing, Applicants submit that the combination of Rune, Mutz, and Hsu fails to teach or suggest the subject matter recited in independent claim 1. Accordingly, claim 1 is patentable over Rune, Mutz, and Hsu under 35 U.S.C. §103(a).

Claims 2 and 3, which depend from independent claim 1 incorporate all of the limitations of independent claim 1 and are, therefore, deemed to be patentably distinct over Rune, Mutz, and Hsu for at least those reasons discussed above with respect to claim 1.

Rejection of claims 4-5 under 35 U.S.C. §103(a)

The Office Action states that the combination of Rune, Mutz, Hsu, and Kostal teaches all of Applicants' recited elements.

As previously discussed, Rune, Mutz, and Hsu fail to teach or suggest the subject matter recited in Applicants' independent claim 1.

Because Rune, Mutz, and Hsu fails to teach or suggest the subject matter recited in amended claim 1, and because Kostal fails to teach or suggest the elements of claim 1 that Rune, Mutz, and Hsu are missing, the addition of Kostal to the reference combination fails to remedy the above-described deficiencies of Rune, Mutz, and Hsu.

Claims 4-5, which depend from independent claim 1, incorporates all of the limitations of independent claim 1 and are, therefore, deemed to be patentably distinct over Rune, Mutz, Hsu, and Kostal for at least those reasons discussed above with respect to independent claim 1.

Conclusion

In view of the foregoing, reconsideration and withdrawal of all rejections, and allowance of all pending claims, are respectfully solicited.

Should the Examiner have any comments, questions, suggestions, or objections, the Examiner is respectfully requested to telephone the undersigned to facilitate an expedited resolution of any outstanding issues.

Respectfully submitted,
COHEN PONTANI LIEBERMAN & PAVANE LLP

By /Alfred W. Froebrich/
Alfred W. Froebrich
Reg. No. 38,887
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: February 5, 2009